DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION
DSTO

DSTO

An Implication of an Optical Data Diode

Malcolm W. Stevens

DSTO-TR-0785

An Implementation of an Optical Data Diode

Malcolm W. Stevens

Information Technology Division
Electronics and Surveillance Research Laboratory

DSTO-TR-0785

ABSTRACT

A data diode is a computer security device that restricts the communication along a network connection between two computers so that data can only be transmitted in one direction. This enables a more sensitive or highly classified computer network to receive data directly from a less secure source while prohibiting the transmission of data in the opposite direction. This paper shows that it is quite simple to construct both the hardware for an optical data diode and also the software to communicate through the device. Data diodes are generally designed to protect the confidentiality of data on the higher classified system. Integrity, availability and reliability issues are also discussed.

An alternate use for data diodes is also explored, where in certain circumstances the data diode can provide strong integrity protection to data on the system which transmits the data through a data diode. The data diode also provides availability protection to this system from the systems on the receiving end of the data diode.

RELEASE LIMITATION

Approved for public release.

DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION
DSTO

Published by

DSTO Electronics and Surveillance Research Laboratory
PO Box 1500
Salisbury, South Australia, 5108

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR-010-857
May 1999

Approved for public release

An Implementation of an Optical Data Diode

Executive Summary

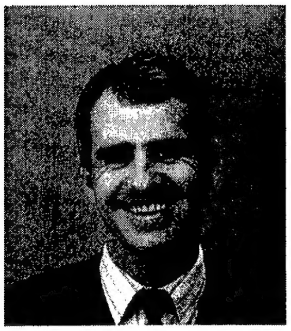
Data diode technology is now at the stage where a data diode can be implemented between networks where there is a requirement for data to be sent from the less classified or sensitive computer network to the more classified network and there is a need to protect the confidentiality of data on the more classified network. In terms of the Defence environment, accreditation for use should be possible at high levels of trust.

This paper shows that it is quite simple to construct the hardware part of the optical data diode from commercial "off the shelf" products. It is also quite simple to implement software which communicates through the data diode and provides electronic mail and file transfer capability. The software model is at the application level and is extensible so that other services such as database replication could be added to the available services through the data diode.

If two networks are at the same classification level but one system is more controlled, with possibly stronger security restrictions, then the data diode can allow data to be transmitted from the more controlled network to the less controlled network while strongly protecting the integrity and availability of the more controlled system. The integrity protection includes protection of the data on the system which sends the data, and also protects against unauthorised system reconfiguration by users or system administrators on the less protected computer system.

If a standard network connection was used the security strength of protection for the more controlled network would be reduced to that of the less controlled network. A firewall could be configured to provide a similar service but it would not have the same strength of protection that the data diode provides.

Author



Malcolm W. Stevens
Information Technology Division

Malcolm Stevens graduated from the University of Adelaide with a Bachelor of Science (Computing and Applied Mathematics) in 1981, and a Bachelor of Science with First Class Honours (Applied Mathematics) in 1982. He then worked as the computing tutor in the Applied Mathematics Department while studying for a Ph. D. (Numerical Modelling of Tides), which was awarded in January 1991. Malcolm joined Trusted Computer Systems Group at DSTO in 1989 where he has been conducting research into computer and network security. Since 1998 Malcolm has been working in the area of Computer Forensics.

Contents

Figures

1. Introduction

A data diode is a computer security device that restricts the communication along a network connection between two points so that data can only be transmitted in one direction. The data diode is configured to guarantee that no data can be passed, either explicitly or covertly, in the opposite direction.

A typical situation where a data diode is useful has a connection between two systems of different classification levels, where data from the lower classified system is to be sent to the higher classified system. This is depicted in Figure 1. Under security restrictions, these networks cannot normally be connected due to the threat of highly classified data being observed by users on the lower classified network.

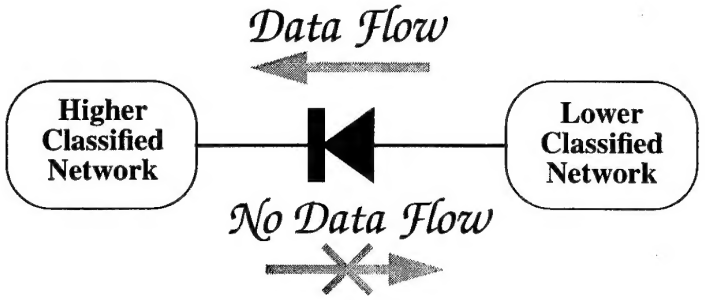


Figure 1 *Depiction of a Data Diode that supplies confidentiality protection to the higher classified network*

2. Previous work on Data Diodes

Previous work [1] on data diodes has been conducted at DSTO where an optical data diode was constructed. The previous work tested a particular configuration and also suggested an alternate design, which was not tested. This paper continues that work by using the suggested alternate design as the basis for the design described in Section 3. Some earlier research on data diodes was carried out in 1988 [2]. In that paper the data diode is called a digital diode.

A group of scientists, at Naval Research Laboratory (NRL) in Washington D.C., have also been working in this area of research and have written several papers: [3], [4] are two of them. The NRL papers describe devices called "Data Pumps" and "Secure Store and Forward Devices". The devices described have two channels of communication, a high volume channel for transporting data from the "Low" network to the "High" network (the upward channel), and a low volume channel for transmitting acknowledgements in the reverse direction (the downward channel). These papers also describe the limiting case of when the acknowledgements channel or downward link has zero bandwidth. This limiting case is what we refer to as the data diode.

The initial work described in [1] observes valid TCP/IP transactions on the lower network and then decides what is relevant to the higher network and passes the data to the relevant destination. This avoids the use of a UDP mechanism but is no more reliable than using UDP transport of data. More recent work has shown that the design described in Section 3. is a viable option. This design uses a UDP transport mechanism to transfer data from the low network to the high network. In the work conducted at NRL and

described in [4], the upward channel of their prototype system also uses a UDP transport mechanism.

The NRL work on data pumps focuses on the packet level in the delivery of data from the low to the high side whereas the work done at DSTO and described in the next section has been demonstrated at the application level. The main idea behind working at the application level was that if human intervention was required to supply information to the low side network about what data was not received properly, then this would be more efficiently achieved at the application level.

3. A Simple Design for an Optical Data Diode

A simple design which has been constructed and demonstrated to work is shown in Figure 2.

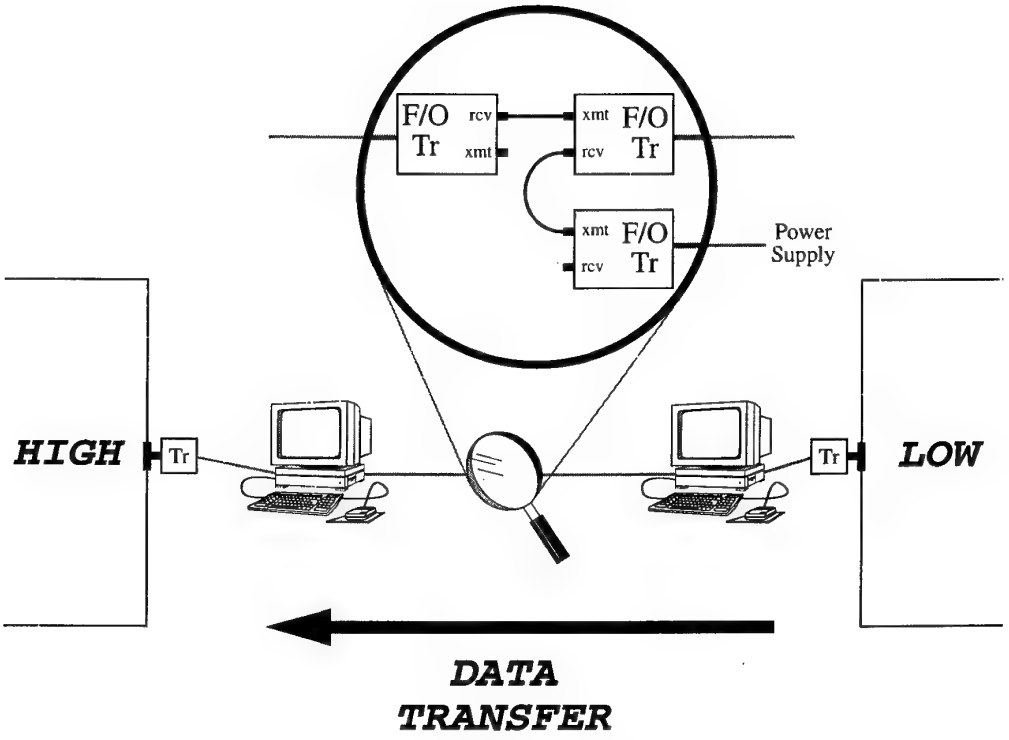


Figure 2 A simple design for an Optical Data Diode

If both the high side and the low side networks already each have a workstation that can be used as a gateway to the other network, then the additional hardware required to implement this design is as listed as follows.

- Three fibre optic transceivers, which each have separate fibre optic lines for transmitting and receiving. This enables the data paths to be separated. The third fibre optic transceiver is required simply to supply a carrier signal to the lower side transceiver which will not work if it does not see the appropriate carrier signal. (This was seen as a cheaper option to modifying the transceiver so that it did not need to see the carrier signal. Using the third transceiver to supply a carrier signal

has the advantage of still being able to purchase "commercial off the shelf" products.)

- Two ethernet cards. One ethernet card is put in each of the gateway workstations so that the two workstations are linked by a dedicated sub-network in order to avoid the possibility of packet collision with other network traffic.
- A power supply for the third fibre optic transceiver. The power for this could be tapped from the cable that connects the other fibre optic transceiver to the low side ethernet card, if this card can supply enough power for two cards.
- Appropriate fibre optic and copper cable to make connections as in Figure 2.

3.1 Advantages of this design

Some of the advantages of this design are listed as follows.

- All the hardware components are commercial "off the shelf" products.
- The design of the optical data diode is very simple. Assurance that it is prohibiting communication in the reverse direction is confirmed by visual inspection of the configuration. It is not entirely clear if a data diode device needs to be evaluated against security criteria but if this is required then it should be quite simple. The evaluation of a data pump would be significantly more difficult.
- The simple design should also enable easy accreditation by the local accrediting authority.
- Such a data diode can be built today without waiting for a product to be developed.

3.2 Disadvantages of this design

The main disadvantage of this design (which is really an inherent problem with data diodes) is the fact that the delivery of data from the low side to the high side is in theory unreliable. In practice it can be very reliable but there is no absolute guarantee that delivery will always occur.

4. The Essential part of an Optical Data Diode

An optical data diode neatly separates into a hardware component and a software component. The configuration of the hardware is entirely responsible for providing confidentiality security. The software is responsible for providing the functionality or services through the one way link. Software such as virus checkers can also be added to provide integrity protection, although this is not at the same high level of assurance as the confidentiality assurance provided by the optical data diode.

4.1 The Hardware

In terms of security the configuration of the hardware component of the optical data diode is the part that is most important. What is required are fibre optic devices which normally communicate to each other through two separate optical fibres. See the representation depicted in Figure 3. Each device uses one fibre to transmit and the other to receive. The devices usually have a light emitting diode at the transmitting end of the fibre and an optical sensor at the receiving end. Each fibre optic devices could be a simple fibre optic transceiver or could be a fibre optic router.

Note: in some fibre optic devices the transmitting device and the receiving device use the same electronic to optical interface thus allowing only one fibre to be used for both directions of data exchange. Such devices are not suitable for use in an optical data diode.

The essential part of the optical data diode is actually the missing optical cable from the transmit port (Xmt) on the left to the receive port (Rcv) on the right in Figure 3. The other optical cable allows communication in the permitted direction. All other hardware components, such as shown in Figure 2, are complementary to the optical cable that allows the low to high communication.

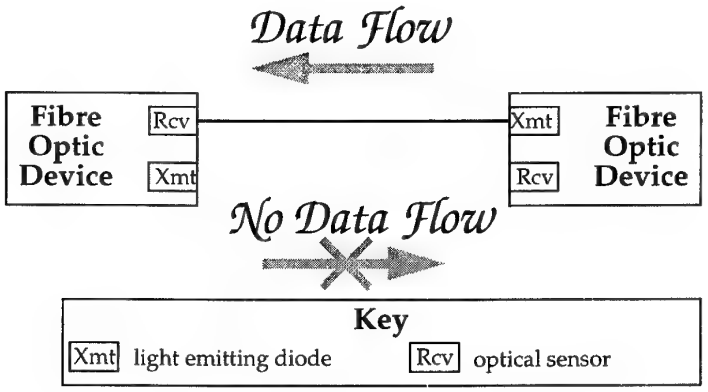


Figure 3 The Essential part of a Data Diode

4.2 Prototype Software for the Data Diode

The physical configuration of the data diode hardware establishes the one way link. The software provides the mechanism for communicating through the link. Most computer communications protocols are bidirectional so that reliability can be achieved. However these protocols cannot be used through a one way connection. UDP, which is one of the TCP/IP suite of protocols, does not require acknowledgments to be sent. A data diode can therefore use the UDP protocol to communicate, through the one way link. However, reliable reception of the transmitted data cannot be absolutely guaranteed. As [4] points out, UDP is an unreliable protocol, but in practice it is very reliable on small dedicated ethernets. The configuration described in Section 3. and depicted in Figure 2 makes use of this by having the data diode on its own separate network thus avoiding the possibility of data collisions with other network traffic.

The reliability of the transmission is dependent on whether the process responsible for receiving data on the high side is able to receive, process and store the transmitted data onto a file system. This process needs to run sufficiently fast to keep up with the throughput and have sufficient buffering to handle unexpected temporary interruptions.

The prototype software was designed to implement the following scheme.

1. Send a small packet of information detailing what is about to be sent, including
   - Type of data sent
   - Length of data
   - Destination of data
   - Origin of data
   - Timing information
   - Serial number uniquely identifying the transmission

2. Send the data through the data diode.

3. Send another small packet of information indicating that the transmission is complete.

If the machine on the high side does not have enough processing power and buffer capacity to receive all the packets sent through the data diode without losing some packets, then the rate at which the data is sent from the low side may need to be slowed down. Of course, it is more desirable to get a more capable machine for the high side receiver but if this is not possible choking the sending rate can be an effective way to increase reliability at the expense of data throughput. For this reason the process responsible for the sending of data has configurable delays between all packets that are sent. If necessary these delays can be increased to retard the sending rate, otherwise they can be minimised to increase throughput.

The two data services that were implemented for this prototype software were chosen as electronic mail (email) delivery and file transfer. The scheme is generic and could be expanded to include other services. The electronic mail service used Simple Mail Transfer Protocol (SMTP).

The prototype software structure is depicted in Figure 4 and the software components that are shown are described as follows.

1. **DiodeMailSend Program**
   This program receives a SMTP mail message from the standard sendmail daemon. (This can be achieved by using the .forward feature). First the program waits for the availability of the lock file then when it is free (i.e. no other program is using the diode) a serial number is obtained. The program then sends an initial packet of information to port number "x" with the details of the mail message, which is about to be sent. The mail message is then sent to the port number corresponding to diode mail delivery (say "x+1"). All details are then recorded in the spooling directory.

2. **DiodeFileSend Program**
   This behaves exactly the same as the DiodeMailSend program except that the program is given the filename of a file to send instead of a mail message.

3. **LockFile**
   The lock file guarantees that only one program can send data at a time. This avoids the possibility of a program transmitting data before another program has finished transmitting, thus avoiding the need for the receiving program to separate different streams of data.

4. **Serial Number Counter**
   There is a unique serial number for each file or email sent (application level).

5. **DiodeReceive Program**
   This program listens on the port "x" for packets informing it of what is about to be delivered. When a message is received the program spawns a child process whose sole task is to process the expected message on the appropriate port number. If it is a file then the file can be placed in a temporary directory to avoid filename clashes and then later delivered to its intended recipient. If it is a mail message it can be delivered straight to the appropriate sendmail daemon. Details of what is received are logged for later checking.

6. **Log Directory**
   Stores the details of each message sent through the diode.

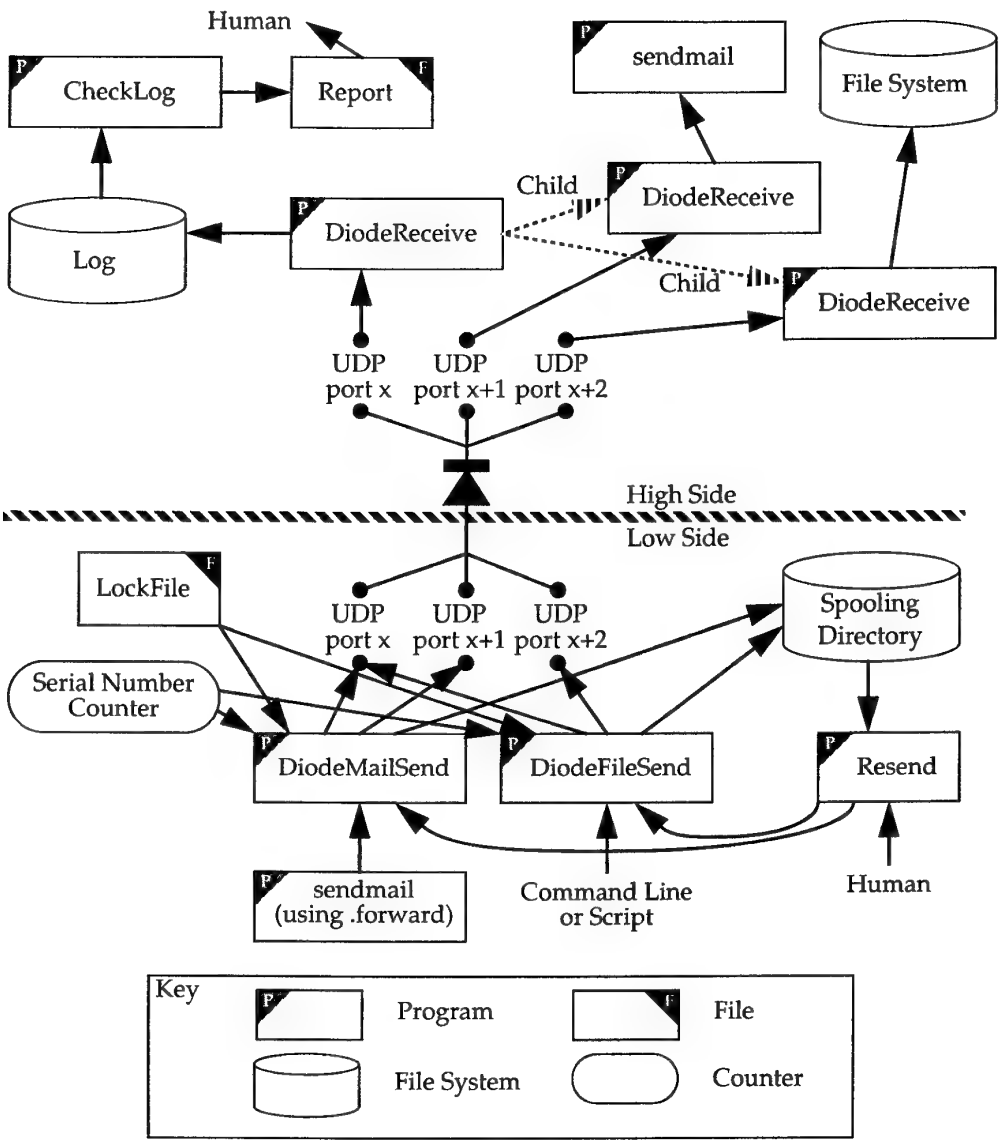


Figure 4 *Prototype Data Diode software configuration*

7. **Spooling Directory**
   Stores the details and possibly contents of data sent through the data diode. Can be cleared when delivery has been confirmed.

8. **CheckLog Program**
   This program scans the log directory and checks for missing or corrupted messages. It compiles a report listing serial numbers to be resent.

9. **Resend Program**
   Given a list of serial numbers this program obtains details from the spooling directory and resends the appropriate data. This program could also clear some of

the contents of the spooling directory if it were told a serial number below which everything has been successfully received.

4.3 Data Diode Services

The physical components of the optical data diode provide the communication link, which is highly assured to be uni-directional.

Any type of service can be implemented through a data diode if it can be modified to work under the restrictions of the uni-directional link.

4.3.1 Electronic Mail and File Transfer

The prototype software described in Section 4.2 implements one particular style of an electronic mail (email) and a file transfer service.

4.3.2 Electronic News

An electronic news service should be relatively easy to implement by making use of the file transfer service.

4.3.3 Web Page Replication

Web sites and web pages can be replicated on the high side by appropriate use of the data diode file transfer mechanism (see 4.3.1). A process running on the low side can send to the high side any desired web pages. This process could also monitor for changes on any of the replicated web pages and then retransmit the new pages to the high side. If desired, content checking could also be performed

4.3.4 Summary of Transfer and Error Notification Service

If reliability is important it may be necessary to implement a summary service. A process on the low side could monitor and list all transactions that are send via the data diode. This process could then periodically sent the list through the data diode to another process on the high side, which has been monitoring all incoming communications. The high side process can then establish if anything has been missed. If the summary is sent at regular intervals then the high side process can even determine if this communication was missing or alternatively could wait until the next summary. Notification of any missing data can be automatically sent, on the high network, to any appropriate persons.

The prototype software described in the previous section partly implements this type of service by using sequential serial numbers, which can be checked on the high side. This also allows for the resending of data that was not correctly transmitted.

4.3.5 Database Replication

One application that is theoretically possible is the replication of a database through a data diode. In its simplest form one could transfer a file representing the entire database through the data diode but in practical terms databases are too large to do this on a regular basis. And unless the content of the database is static this could not happen often enough to keep the replicated copy up to data.

Many commercially available databases have mechanisms for replication of part or all of a database, but these usually require synchronous two way communication between the main database server and the replication server.

In order for database replication to be achievable through a data diode the replication of the database needs to happen asynchronously and without acknowledgements back to the main database. Once a copy of the database has been established on the high side network, then changes made to the main database could be recorded and transmitted to

the high side replication. A process on the high side network would then need to process the received changes by making the same changes to the replicated copy.

Mechanisms to handle possible transmission loss would need to be considered.

5. Assurance of a Data Diode

The assurance of a data diode measures the strength of guarantee that the data diode will behave in the expected manner and can be trusted to do so. The assurance levels E0 to E6 of the Information Technology Security Evaluation Criteria (ITSEC) [5] can be used to measure the assurance of a data diode. The configuration described in Section 3. and depicted in Figure 2 should be able to satisfy very high assurance levels for confidentiality assurance.

5.1 Confidentiality Risks in using a Data Diode

The data diode is specifically designed to protect the confidentiality of data on the high side computer system. This is the data diode's main objective. The data diodes assurance for protecting confidentiality relies on the following two facts:

1. There is no fibre optic link between the transmit port of the transceiver on the receiving side of the data diode and the receiving port of the transceiver on the transmitting side of the data diode. This is a physical characteristic that can be verified visually.

2. The transceiver on the receiving side of the data diode has not been tampered with. Or more specifically, the detecting diode of the receiving port of this transceiver has not been replaced with a component that can both transmit and receive. This should be easily verifiable.

If both the above facts can be verified then the correct operation of the data diode is assured to a very high level.

The part that guarantees the high level of trust is the fact that light is not being transmitted from the transceiver on the high side to the transceiver on the low side and therefore no data can be transferred. All the other parts of the data diode do not have to be trusted. Even if there is malicious software on both the high and low systems, the confidentiality of the high side data is maintained. Of course in this situation one might also be concerned for the integrity and availability of the data on the high side system.

5.2 Integrity and Availability on the High Side (Receiving)

As previously discussed, the principal design criteria of a data diode is to protect the confidentiality of data on the high side computer system. Connecting two networks together with a data diode also exposes the higher classified network to a threat of either a denial of service attack (availability) or an integrity attack.

This section considers the availability and integrity of the high side system, which is the system which receives data through the data diode.

These threats are not unique to data diodes but apply to any means of importing information or data onto a computer system. Protection against these threats is achieved by the same methods that are applied to any data that is imported.

Denial of service and integrity threats could be realised by an attack which is implemented by importing machine code executable images onto the higher classified network and then, by some means, having these executables run on the network. This attack cannot violate the confidentiality of the system or any data on it but it could

possibly destroy or manipulate the system or data or overload the system to create a denial of service attack. A computer virus is an example of such malicious code. There is a smaller class of threats, that is becoming increasingly common, which could be realised through the importing of data files which contain a virus, such as Word 6.0 files which contain viral data which affects the operation the Word 6.0 program through the macro facility (commonly known as macro viruses).

While not strictly part of the data diode, measures can be incorporated in conjunction with the data diode configuration which can help reduce the risk of availability and integrity attacks.

Two components that could be used with data diodes are listed below and depicted in Figure 5.

1. Packet Filters
2. Integrity and Virus Checkers

These are discussed in more detail in the following section. Configuration of these components is not all that security critical and could depend on the resources that are available. Packet filtering can be done by many commercially available routers and integrity and virus checking could be done on the high side computer if it had enough processing power so that reliability of data transfer was not affected. Some commercially available "firewalls" could supply the required functionality.

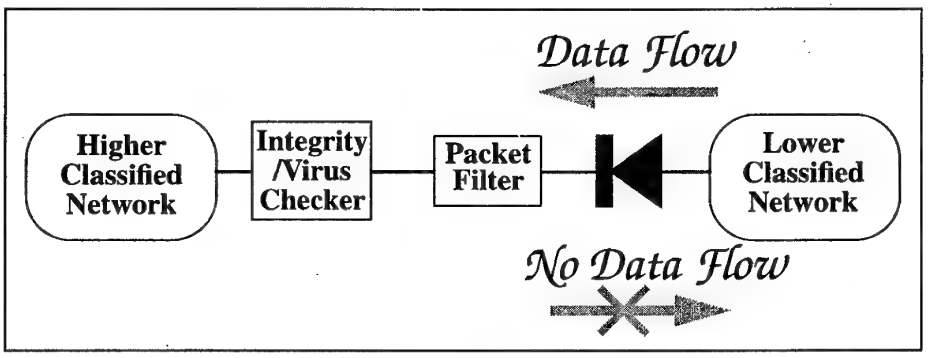


Figure 5 *Other Components that could be used with a Data Diode*

5.3 Maximising Reliability

There are numerous ways to minimise the effect of the unreliable transport mechanism depending on the severity of the consequences and the resources that are available. Some of the strategies that could be considered are as follows.

- Making sure that the workstation on the high side has enough processing power and storage so that it can listen and transfer any incoming data to a stable buffer at a faster rate than the sending rate from the low side. This may include an adequate buffer size in order to smooth out peak data transmission rates.
- On the high machine, increasing the size of the kernel network buffers and adjusting the process priorities so that the listening function is carried out with a high priority and with enough buffer space to cope with short delays. Experiments by [6] have shown that if this is done data transfer rates are achievable up to 98% of the theoretical bandwidth of the 10 Mbps without loss of data.

- Using some sort of forward error correction mechanism so that missing data can be reconstructed. (A simple form of error correction is the duplication of data sent from the low side. This of course halves the available bandwidth.)
- Software assisted detection of missing data. If the low side sending process sequentially numbers the data sent then software on the high side, on receipt of a subsequent message, can detect that there was a missing message. This enables a list of missing data to be compiled on the high side. If this is communicated to the low side (not electronically as that would provide a possible covert channel) then the data could be resent.

6. Integrity and Availability Protection for the Sending Network

6.1 Introduction

Data diodes are often used to supply highly trusted protection to the confidentiality of data on a computer system, where data from the lower classified system is to be sent to the higher classified system. This is depicted in Figure 1. Under security restrictions, these networks cannot use standard network connections due to the threat of highly classified data being observed by users on the lower classified network.

It is proposed that, in situations where **the two networks are at the same classification levels**, then the data diode can provide highly trusted integrity and availability protection to the computer system which sends the data. This situation is depicted in Figure 6.

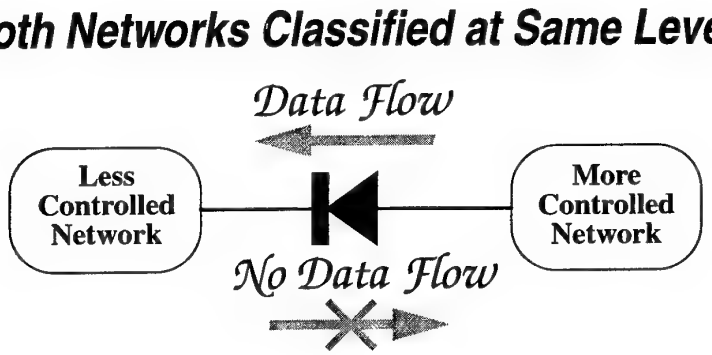


Figure 6 *Depiction of a Data Diode that supplies integrity protection to the more controlled computer system.*

6.2 Integrity Properties of Data Diodes

This section discusses integrity and availability protection that a data diode can provide to the computer system that sends the data through the data diode. The integrity protection that the sending system is provided with, covers the integrity of the data on the computer system and also protection against unauthorised configuration of the computer system from the system that receives the data. (Note: the protection that is provided is not a general protection but a specific protection against attacks from the

receiving computer system. The protection is not provided for any other network connections to the system that sends the data that do not use a data diode.)

Consider the situation where a data diode connects two computer networks which are at different security classifications, such as the situation depicted in Figure 1. The data diode provides integrity and availability protection to the less classified system from the more classified system. This is usually of little importance as one is usually more interested in maintaining the availability and integrity of the higher classified system. Integrity and availability issues of the higher classified system (or receiving system) have been discussed in Section 5.2.

Data diodes are usually not connected to allow data to be transferred from high to low because there is a large risk that sensitive data on the high network, which is not allowed or desired on the low network, will be sent through the data diode, either accidentally or maliciously, possibly by some hostile code executing without human consent.

The situation that is of interest is where the two networks handle data which is at the same classification level. This is of interest when the two networks are not normally connected because one of the networks is more controlled than the other. Figure 6 depicts such a situation. Examples of network architectures where such a connection may be useful are given in Section 6.3

The mechanism that transports data through the data diode is a "push" mechanism. So it is totally at the discretion of the sending system as to what data is sent to the less protected system.

Due to the one way flow of data it would be impossible for anyone, even system administrators, on the less controlled network to "hack" into the more controlled network through the data diode.

Users on the less controlled network could have access to data from the more controlled network, if someone on the more controlled network initiated a data transfer. Users on the less controlled network then have access to a copy of the original data. Thus the users on the less controlled network can not affect the integrity of any data on the more controlled network, even if they have uncontrolled access to a copy of the data.

A firewall could be configured to provide a similar service to the data diode but it would not have the same strength of protection as the data diode. The number of bugs in firewall implementations, as can be seen in bug lists, such as that distributed by BUGTRAQ@NETSPACE.ORG, indicate the generally level of protection provided by most firewalls. Firewall protection is generally recognised as being better than using a direct connection with no firewall but the protection that they provide will probably never be assured to a high level of trust and may never be completely invulnerable.

6.3 Examples of Use

The next three sub-sections give possible examples where a data diode may be used to provide integrity and availability protection to the network which sends the data through a data diode.

6.3.1 More Controlled Network

A more controlled network may have stricter security policies concerning the importing of data or over what software can be used. On this type of system, users may only be able to run software from a certain set of alternatives. There may need to be strict control over any imported data to check for malicious intent in executable code or macro viruses. These strict requirements may not necessarily apply to some other network at the same classification level that may have a need to receive data from the more controlled network.

If a standard network connection was used to pass data from the more controlled network to the less controlled network then the security mechanisms for the combined system are reduced to the lowest common denominator. This would not be in the best interest of the more controlled network.

Commercial enterprises may have computer systems that fall into this category, for example companies in the banking sector. Selected information from a highly controlled enterprise system could be transmitted to a more accessible system. This information could then be made available to management, regulatory officials, staff and even customers without jeopardising the integrity of the data on the highly protected enterprise system.

Access control policies, which distinguish between who can read data and who can write data, could even be implemented in this way.

A data diode connection as shown in Figure 7 allows the transfer of data and maintains the stricter network policy control in the more controlled network.

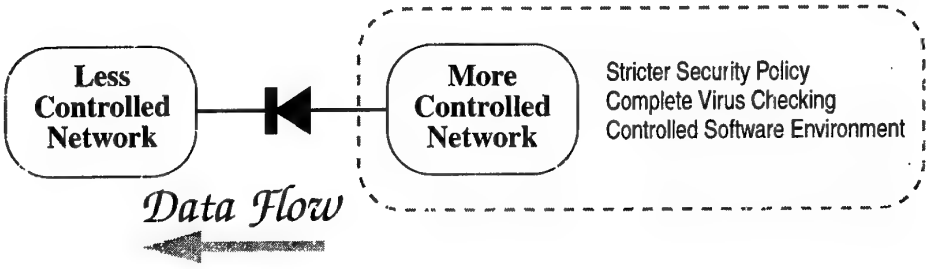


Figure 7 Data Diode Providing Integrity Protection

6.3.2 Integrity Protection for a Database

Another situation where this type of data diode may be used is where some data has a "sovereignty restriction" placed on it's integrity. That is, the owners of the data are responsible for the integrity and currency of a data base but allow other computer systems of the correct classification levels to access the data.

A data diode connection as shown in Figure 8 could allow data to be copied from one network to the other allowing the receiving network users access to the data while the sending network still maintains control over the data including the data's integrity and currency.

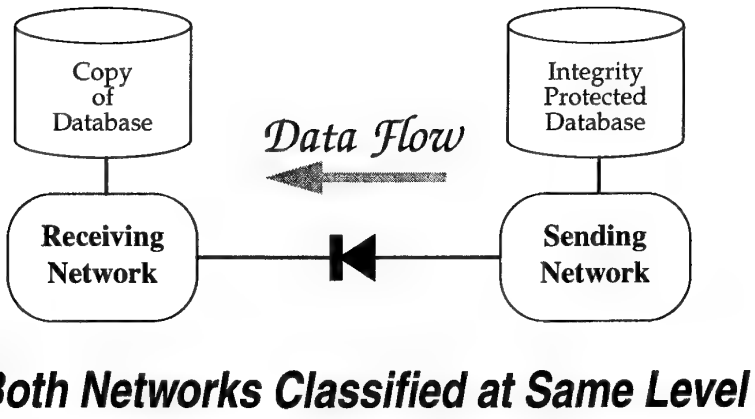


Figure 8 Integrity protection for a Database

6.3.3 Remote Foreign Node

In this situation (see Figure 9) the data diode can provide very strong integrity protection including reconfiguration protection for the foreign system including the remote node.

The data diode connection allows data to be electronically sent from the remote node to the local system.

The remote node can be remotely configured and controlled from the main foreign system without the possibility of interference from the local system.

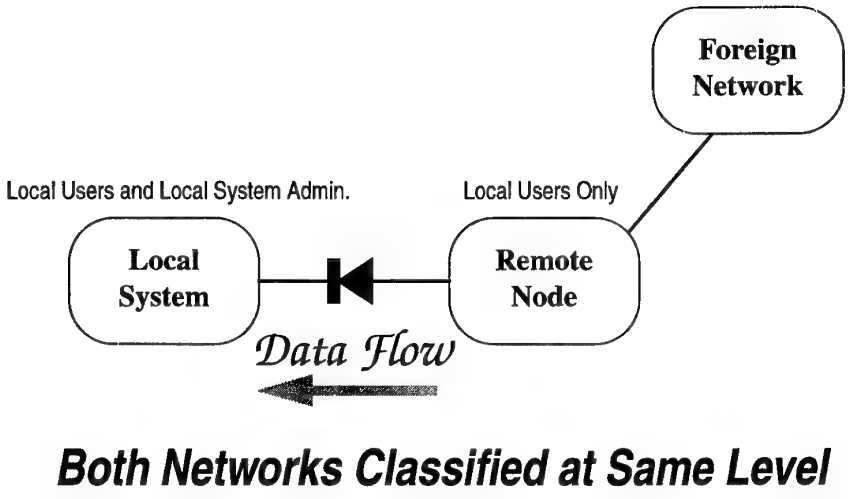


Figure 9 Data Transfer from Foreign System

6.4 Strength of Protection

The configuration of a data diode as described in Section 3. should be able to satisfy very high assurance levels for confidentiality assurance (see Section 5.). Thus the configurations described in this section should be able to satisfy very high assurance levels for integrity and availability assurance.

7. Mechanisms to Reduce Information Security Risks

7.1 Physical Protection

Since a data diode is essentially a one way path between two networks and it is assumed that the two networks have differing security requirements, the data diode usually needs to be physically protected to avoid the threat of reconfiguration or bypass.

7.2 Packet Filters

The prototype software described in Section 4.2 communicates UDP packets to specific port numbers on the high side computer. Packet filtering can be set up to stop any communication to port numbers other than those used by the data diode software. This stops any non data diode software being able to send data to the high side network. This helps integrity, availability and reliability. Thus the only data that could be transmitted would be on the port numbers allocated to the data diode software. It would be possible to configure the data diode software so that if a non diode packet is detected then a set of predetermined actions is taken.

Packet filtering can be achieved by many commercially available routers. Some of these even have mechanisms to record occurrences of filtered out packets.

7.3 Integrity/Virus Checking

Programs, which routinely and automatically filter any incoming data which comes through the data diode, can be written. There are many virus checkers commercially available. These programs check for viruses, data files that have embedded macro commands, java applets or any other threat that is appropriate to guard against. If the threat of such attacks was considered to be significant, then policies could be implemented that prevent the execution of any code imported through the data diode.

Once a specific threat has been identified, then if it considered significant enough, measures can be introduced to detect, warn and remove such infected files or data.

It would usually be necessary to have discussions with the authority responsible for the accreditation of the computer security for the system, in order to assess the magnitude of the possible threats and the available countermeasures that may be required to minimise the risk of integrity or denial of service problems.

8. Summary

This paper shows that data diodes are easily constructed and software to communicate through them is relatively simple to write.

The data diode is designed to protect the confidentiality of data on the high side network. It achieves this with a high level of assurance. Measures can also be taken to reduce the risk of loss of integrity and availability to the receiving network.

The paper [6] shows that the UDP communication through a data diode can be both high throughput and high reliability if adequate resources and priorities are met.

Data diodes also provide integrity and availability protection to the network which transmits through a data diode. This is normally not required but in certain circumstances it can be used as an important part of a security implementation.

Data diode technology is now at a stage where there are no technical issues preventing their implementation. If anyone has a need to construct such a service between two networks, then it is quite simple to achieve and should achieve accreditable operation.

9. REFERENCES

[1] Stevens M. and Pope M. *Data Diodes.* Electronics and Surveillance Research Laboratory (DSTO), Technical Report - DSTO-TR-0209, July 1995.

[2] Cohen F. *Designing Provably Correct Information Networks with Digital Diodes.* Computers & Security, Volume 7, pages 279-286, 1988.

[3] Froscher J. N., Goldschlag D. M., Kang M. H., Landwehr C. E., Moore A., Moskowitz I. S. and Payne C. N. *Improving Inter-Enclave Information Flow for a secure Strike Planning Application.* Proceedings of the 11th Annual Computer Security Applications Conference, New Orleans, Louisiana, December 1995.

[4] Goldschlag D. M. *Several Secure Store and Forward Devices.* Proceedings of the Third ACM Conference on Computer and Communications Security, New Delhi, India, March 1996.

[5] European Communities - Commission. *Information Technology Security Evaluation Criteria (ITSEC) Provisional Harmonised Criteria,* Version 1.2, ISBN 92-826-3004-8, Catalogue number CD-71-91-502-EN-C, June 1991.

[6] Yesberg J. D. and Klink M. W. *An Investigation into the Reliability of User Datagram Protocol Reception for a Data Diode.* Electronics and Surveillance Research Laboratory (DSTO), Technical Report - DSTO-TR-0649, April 1998.

An Implementation of an Optical Data Diode

M. Stevens

(DSTO-TR-0785)

DISTRIBUTION LIST

	Number of Copies
AUSTRALIA	
DEFENCE ORGANISATION	
Task sponsor:	
Director General, Command, Control, Communication and Intelligence Development	1
S&T Program	
Chief Defence Scientist)	
FAS Science Policy)	1 shared copy
AS Science Corporate Management)	
Director General Science Policy Development	1
Counsellor, Defence Science, London	Doc Control Sheet
Counsellor, Defence Science, Washington	Doc Control Sheet
Scientific Adviser - Policy and Command	1
Navy Scientific Adviser	1 copy of Doc Control Sheet and 1 distribution list
Scientific Adviser - Army	Doc Control Sheet and 1 distribution list
Air Force Scientific Adviser	1
Director Trials	1
Aeronautical & Maritime Research Laboratory	
Director	1
Electronics and Surveillance Research Laboratory	
Director	1
Chief Information Technology Division	1
Research Leader Command & Control and Intelligence Systems	1
Research Leader Military Computing Systems	1
Research Leader Command, Control and Communications	1
Executive Officer, Information Technology Division	Doc Control Sheet
Head, Information Architectures Group	1
Head, Information Warfare Studies Group	1
Head, Software Systems Engineering Group	Doc Control Sheet
Head, Year 2000 Project	Doc Control Sheet
Head, Trusted Computer Systems Group	1
Head, Advanced Computer Capabilities Group	1
Head, Systems Simulation and Assessment Group	Doc Control Sheet

Head, Distributed Systems Group	1
Head, C3I Systems Concepts Group	1
Head Organisational Change Group	1
Head, C3I Operational Analysis Group	Doc Control Sheet
Head Information Management and Fusion Group	Doc Control Sheet
Head, Human Systems Integration Group	Doc Control Sheet
Head, C2 Australian Theatre	1
Malcolm Stevens (ACC Group) (Author)	1
Publications and Publicity Officer, ITD	1

DSTO Library and Archives

Library Fishermens Bend	1
Library Maribyrnong	1
Library Salisbury	2
Australian Archives	1
Library, MOD, Pyrmont	Doc Control Sheet

Capability Development Division

Director General Maritime Development	Doc Control Sheet
Director General Land Development	Doc Control Sheet
Director General C3I Development	Doc Control Sheet
Director General Aerospace Development	Doc Control Sheet

Navy

SO (Science), Director of Naval Warfare, Maritime Headquarters Annex, Garden Island, NSW 2000.	1

Army

ABCA Office, G-1-34, Russell Offices, Canberra	4
SO (Science), DJFHQ(L), MILPO, Enoggera, Qld 4051	Doc Control Sheet
NAPOC QWG Engineer NBCD c/- DENGRS-A, HQ Engineer Centre Liverpool Military Area, NSW 2174	Doc Control Sheet

Intelligence Program

DGSTA Defence Intelligence Organisation	1

Corporate Support Program (libraries)

OIC TRS Defence Regional Library, Canberra	1
US Defence Technical Information Center	2
UK Defence Research Information Centre	2
Canada Defence Scientific Information Service	1
NZ Defence Information Centre	1
National Library of Australia	1

Universities and Colleges

Australian Defence Force Academy	1
Library	1
Head of Aerospace and Mechanical Engineering	1

Deakin University, Serials Section (M list)), Deakin University Library, Geelong, 3217	1
Senior Librarian, Hargrave Library, Monash University	1
Librarian, Flinders University	1

Other Organisations

NASA (Canberra)	1
AGPS	1
State Library of South Australia	1
Parliamentary Library, South Australia	1

OUTSIDE AUSTRALIA

Abstracting and Information Organisations

Library, Chemical Abstracts Reference Service	1
Engineering Societies Library, US	1
Materials Information, Cambridge Scientific Abstracts	1
Documents Librarian, The Center for Research Libraries, US	1

Information Exchange Agreement Partners

Acquisitions Unit, Science Reference and Information Service, UK	1
Library - Exchange Desk, National Institute of Standards and Technology, US	1
SPARES	5
Total number of copies:	62

Page classification: UNCLASSIFIED

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

An Implementation of an Optical Data Diode

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document (U)
Title (U)
Abstract (U)

4. AUTHOR(S)

Malcolm W. Stevens

5. CORPORATE AUTHOR

Electronics and Surveillance Research Laboratory
PO Box 1500
Salisbury SA 5108

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TR-0785	AR-010-857	Technical Report	May 1999

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
N9505/13/151	ADF 96/178	DGC3ID	30	6

13. DOWNGRADING/DELIMITING INSTRUCTIONS

N/A

14. RELEASE AUTHORITY

Chief, Information Technology Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for Public Release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE CENTRE, DIS NETWORK OFFICE, DEPT OF DEFENCE, CAMPBELL PARK OFFICES, CANBERRA ACT 2600

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CASUAL ANNOUNCEMENT Yes

18. DEFTEST DESCRIPTORS

Diodes
Optical data
Computer security

19. ABSTRACT

A data diode is a computer security device that restricts the communication along a network connection between two computers so that data can only be transmitted in one direction. This enables a more sensitive or highly classified computer network to receive data directly from a less secure source while prohibiting the transmission of data in the opposite direction. This paper shows that it is quite simple to construct both the hardware for an optical data diode and also the software to communicate through the device. Data diodes are generally designed to protect the confidentiality of data on the higher classified system. Integrity, availability and reliability issues are also discussed.

An alternate use for data diodes is also explored, where in certain circumstances the data diode can provide strong integrity protection to data on the system which transmits the data through a data diode. The data diode also provides availability protection to this system from the systems on the receiving end of the data diode.